

What is claimed is:

1 1. A data administration method, which comprises:

2 preparing a real data section by encrypting digital
3 content to be distributed;

4 preparing a header data section provided with symbol
5 information symbol-converted for visual or auditory
6 recognition of attributes of the digital content;

7 preparing a consent-information-added header data
8 section in which consent information containing information
9 on a content key used as an encryption key in encrypting the
10 digital content is embedded in the header data section as an
11 electronic watermark; and

12 preparing composite data in which the real data section
13 and the consent-information-added header data section are
14 composited, and distributing the composite data.

1 2. The data administration method as set forth in claim
2 1, wherein said header data section is made by compositing
3 into one image data item more than one image-symbol data
4 item symbol-converted for visually recognizing attributes
5 corresponding respectively to a plurality of digital content
6 items.

1 3. A data administration method, which comprises:

2 preparing a real data section by encrypting digital
3 content to be distributed;

4 preparing a header data section enabling visual or
5 auditory recognition of substance of the digital content;
6 preparing a consent-information-added header data
7 section in which consent information containing information
8 on a content key used as an encryption key in encrypting the
9 digital content is embedded in the header data section as a
10 visually or auditorily unrecognizable electronic watermark;
11 preparing an annex data section in which use
12 restriction information for restricting use of the digital
13 content is encrypted;
14 preparing composite data by compositing the real data
15 section and the consent-information-added header data
16 section, simultaneously compositing the annex data section;
17 and
18 distributing the composite data.

1 4. The data administration method as claimed in claim
2 3, wherein the use restriction information is embedding
3 logic for embedding the consent information as the
4 electronic watermark in the header data section.

1 5. The data administration method as set forth in claim
2 3, wherein the use restriction information is based on a use
3 term during which, or on a use count up to which, the
4 digital content is usable.

1 6. The data administration method as set forth in claim
2 3, wherein the use restriction information is encrypted

3 with, as an encryption key, personal information on a user
4 of the digital content.

1 7. The data administration method as set forth in claim
2 6, wherein the encryption key when encrypting the use
3 restriction information is a password preset by the user.

1 8. The data administration method as set forth in claim
2 6, wherein the encryption key when encrypting the use
3 restriction information is identifying information specific
4 to a recording medium in which the composite data is
5 recorded.

1 9. The data administration method as set forth in claim
2 6, wherein the encryption key when encrypting the use
3 restriction information is vital information on the user.

1 10. A data administration method, which comprises:
2 separating an annex data section from composite data
3 distributed as a composite of

4 a real data section in which digital content to be
5 distributed is encrypted,

6 in a header data section enabling visual or
7 auditory recognition of substance of the digital
8 content, a consent-information-added header data
9 section in which consent information containing
10 information on a content key used as an encryption key
11 in encrypting the digital content is embedded as a

12 visually or auditorily unrecognizable electronic
13 watermark, and
14 an annex data section in which use restriction
15 information for restricting use of the digital content
16 is encrypted;
17 decrypting the annex data section and extracting the
18 use restriction information;
19 extracting the consent information embedded in the
20 consent-information-added header data section based on the
21 use restriction information;
22 obtaining from the consent information a content key
23 for decrypting the digital content; and
24 using the content key, decrypting the real data section
25 into its original digital content to allow use by users.

1 11. A data administration method characterized by:
2 preparing a real data section by encrypting digital
3 content to be distributed;
4 preparing a header data section enabling visual or
5 auditory recognition of substance of the digital content;
6 preparing a consent-information-added header data
7 section in which consent information containing information
8 on a content key used as an encryption key in encrypting the
9 digital content is embedded in the header data section as a
10 visually or auditorily unrecognizable electronic watermark;

11 embedding in the header data section as a visually or
12 auditorily unrecognizable electronic watermark a hash value
13 generated from the real data section using a hash function;
14 and thereafter

15 preparing composite data in which the real data section
16 and the consent-information-added header data section are
17 composited, and distributing the composite data.

1 12. A data administration method characterized by:

2 preparing a real data section by encrypting digital
3 content to be distributed;

4 preparing a header data section enabling visual or
5 auditory recognition of substance of the digital content;

6 preparing a consent-information-added header data
7 section in which consent information containing information
8 on a content key used as an encryption key in encrypting the
9 digital content is embedded in the header data section as a
10 visually or auditorily unrecognizable electronic watermark;
11 and

12 decrypting the real data section into digital content
13 for sending out, by line-connecting to a predetermined
14 contact destination, content information from the digital
15 content that is decrypted, and therein

16 embedding in the header data section as a visually
17 or auditorily unrecognizable electronic watermark the
18 content information from the digital content that is

19 decrypted and information on the predetermined contact
20 destination; and thereafter

21 preparing composite data in which the real data
22 section and the consent-information-added header data
23 section are composited, and distributing the composite
24 data.

1 13. A data administration method characterized by:

2 preparing a real data section by encrypting digital
3 content to be distributed;

4 preparing a header data section enabling visual or
5 auditory recognition of substance of the digital content;

6 preparing a consent-information-added header data
7 section in which consent information containing information
8 on a content key used as an encryption key in encrypting the
9 digital content is embedded in the header data section as a
10 visually or auditorily unrecognizable electronic watermark;

11 preparing composite data in which the real data section
12 and the consent-information-added header data section are
13 composited, and therein retaining within the composite data
14 record-location information from a server in which the
15 digital content is registered; and

16 distributing the composite data.

1 14. The data administration method as set forth in

2 claim 13, characterized in that the record-location

3 information from the server in which the digital content is

4 registered is embedded in the header data section as a
5 visually or auditorily unrecognizable electronic watermark.

1 15. A data administration method characterized by:

2 preparing a real data section by encrypting digital
3 content to be distributed;

4 preparing a header data section enabling visual or
5 auditory recognition of substance of the digital content;

6 preparing a consent-information-added header data
7 section in which consent information containing information
8 on a content key used as an encryption key in encrypting the
9 digital content is embedded in the header data section as a
10 visually or auditorily unrecognizable electronic watermark;
11 and

12 preparing composite data in which the real data section
13 and the consent-information-added header data section are
14 composited, and therein retaining within the composite data
15 vital template information generated based on vital
16 information on a user of the digital content; and

17 distributing the composite data.

1 16. The data administration method as set forth in

2 claim 15, characterized in that the vital template
3 information is embedded in the header data section as a
4 visually or auditorily unrecognizable electronic watermark.

1 17. A data administration method characterized by:

2 preparing a real data section by encrypting digital
3 content to be distributed;

4 preparing a header data section enabling visual or
5 auditory recognition of substance of the digital content;

6 preparing a consent-information-added header data
7 section in which consent information containing information
8 on a content key used as an encryption key in encrypting the
9 digital content, and identifying information specific to a
10 recording medium for recording the digital content, are
11 embedded in the header data section as a visually or
12 auditorily unrecognizable electronic watermark; and

13 preparing composite data in which the real data section
14 and the consent-information-added header data section are
15 composited, and distributing the composite data.

1 18. A data administration method characterized by:

2 preparing a real data section by encrypting digital
3 content to be distributed;

4 preparing a header data section enabling visual or
5 auditory recognition of substance of the digital content;

6 preparing a consent-information-added header data
7 section in which consent information containing information
8 on a content key used as an encryption key in encrypting the
9 digital content, and a control code allowing a given
10 operation on an information device for reproducing the
11 digital content, are embedded in the header data section as

12 a visually or auditorily unrecognizable electronic

13 watermark; and

14 preparing composite data in which the real data section
15 and the consent-information-added header data section are
16 composited, and distributing the composite data.

1 19. A data administration method, which comprises:

2 preparing a real data section by encrypting digital
3 content to be distributed;

4 preparing a header data section enabling visual or
5 auditory recognition of substance of the digital content;

6 preparing a consent-information-added header data
7 section in which consent information containing information
8 on a content key used as an encryption key in encrypting the
9 digital content is embedded in the header data section as a
10 visually or auditorily unrecognizable electronic watermark;
11 and

12 preparing composite data by compositing the real data
13 section and the consent-information-added header data
14 section, and distributing the composite data; characterized
15 in that

16 privileges information for the digital content
17 including copyright information is embedded within the
18 digital content as an electronic watermark.

1 20. The data administration method as set forth in
2 claim 19, characterized in that morphology and code level of

3 the electronic watermark embedded in the digital content are
4 determined based on a data quality level and a security
5 level required by the digital content.

1 21. The data administration method as set forth in
2 claim 19, characterized in that the electronic watermark
3 embedding mode in the digital content differs from the
4 electronic watermark embedding mode in the header data
5 section.